Lect.7

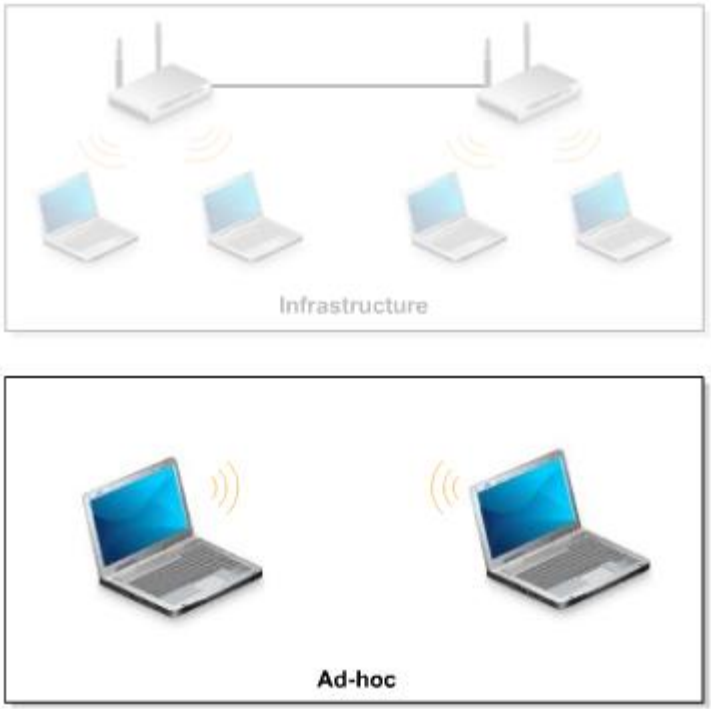
IEEE 802.11 Wireless Local Area Networks (RF-LANs)

Wireless?

- A wireless LAN or WLAN is a wireless local area network that uses radio waves as its carrier.
- The last link with the users is wireless, to give a network connection to all users in a building or campus.
- The backbone network usually uses cables

Types of Wireless LANs

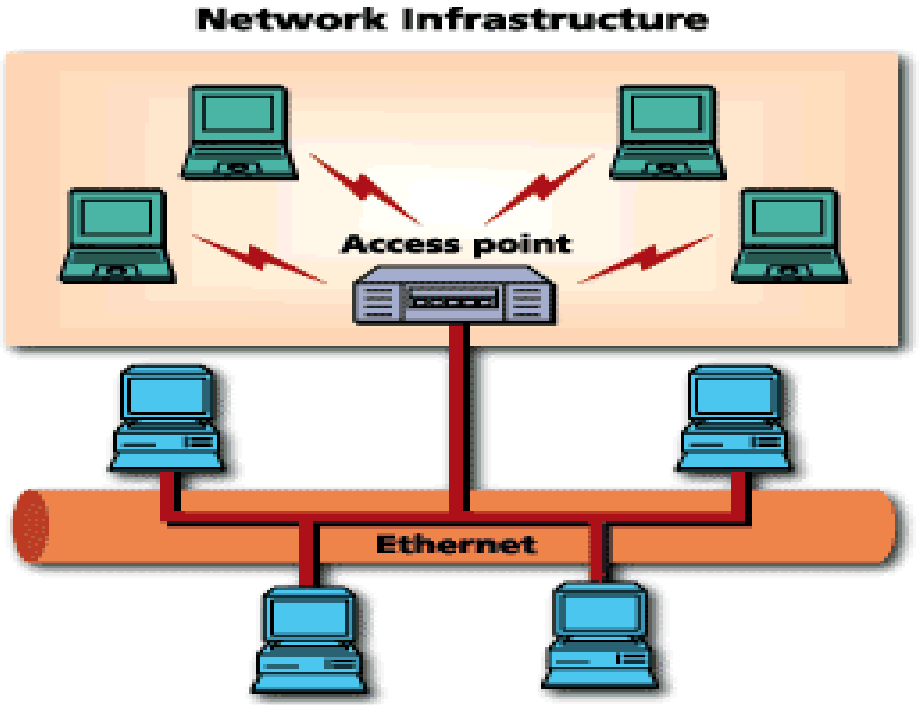
- Infrastructure
- Ad-hoc



Common Topologies

(Infrastructure) The wireless LAN connects to a wired LAN

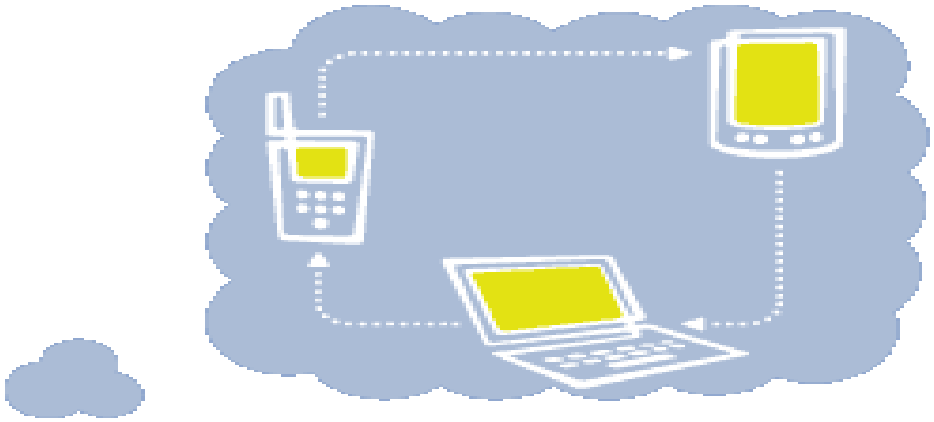
- There is a need of an access point that bridges wireless LAN traffic into the wired LAN.
- The access point (AP) can also act as a repeater for wireless nodes, effectively doubling the maximum possible distance between nodes.



Common Topologies

(Ad hoc) Complete Wireless Networks

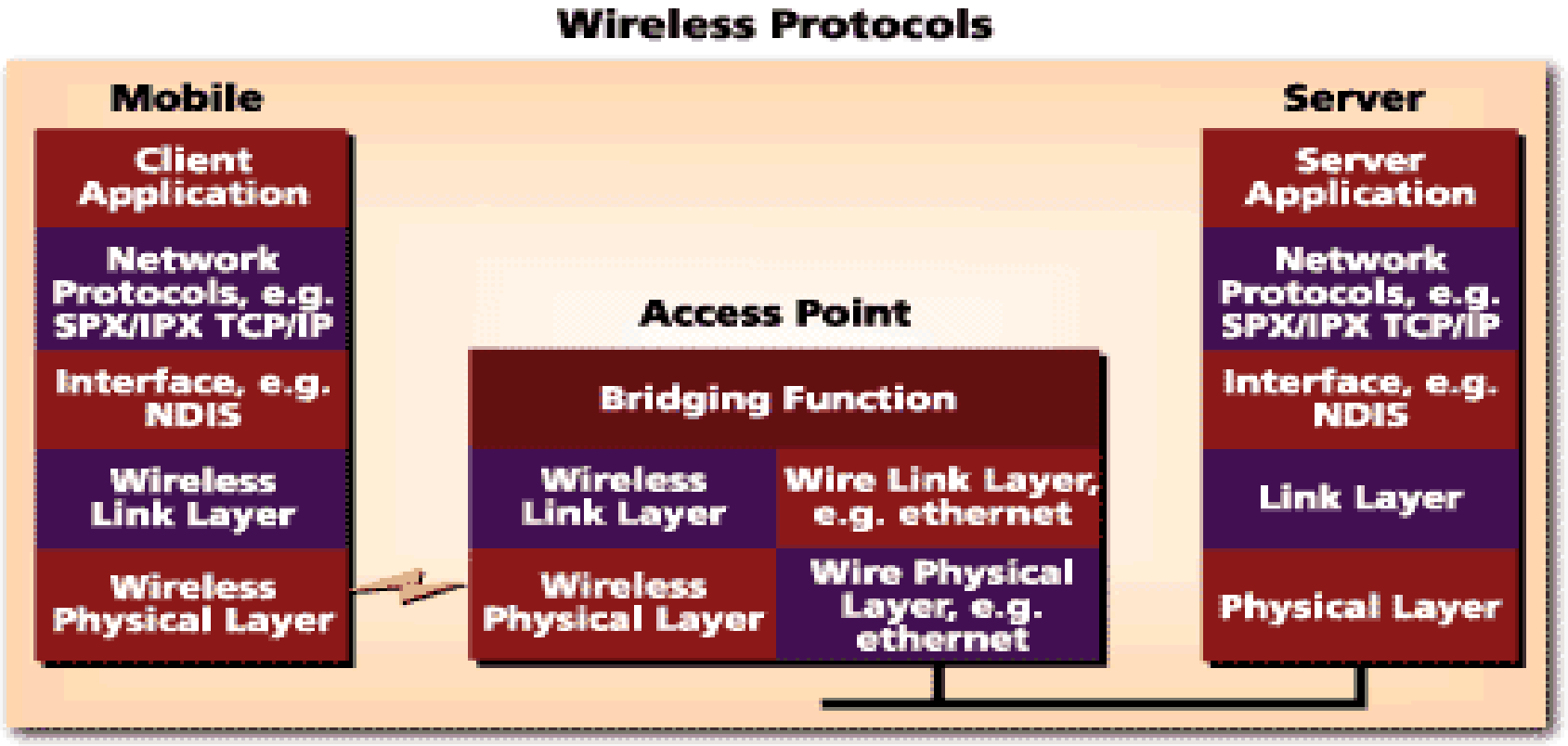
- The physical size of the network is determined by the maximum reliable propagation range of the radio signals.
- Referred to as **ad hoc** networks
- Are self-organizing networks without any centralized control
- Suited for temporary situations such as meetings and conferences.



Integration With Existing Networks

- Wireless Access Points (APs) - a small device that bridges wireless traffic to your network.
- Most access points bridge wireless LANs into Ethernet networks, but Token-Ring options are available as well.

Integration With Existing Networks



How are WLANs Different?

- They use specialized **physical and data link** protocols
- They integrate into existing networks through **access points** which provide a bridging function
- They let you stay connected as you **roam** from one coverage area to another
- They have unique **security** considerations
- They require **different hardware**
- They offer **performance** that differs from wired LANs.

Physical and Data Link Layers

Physical Layer:

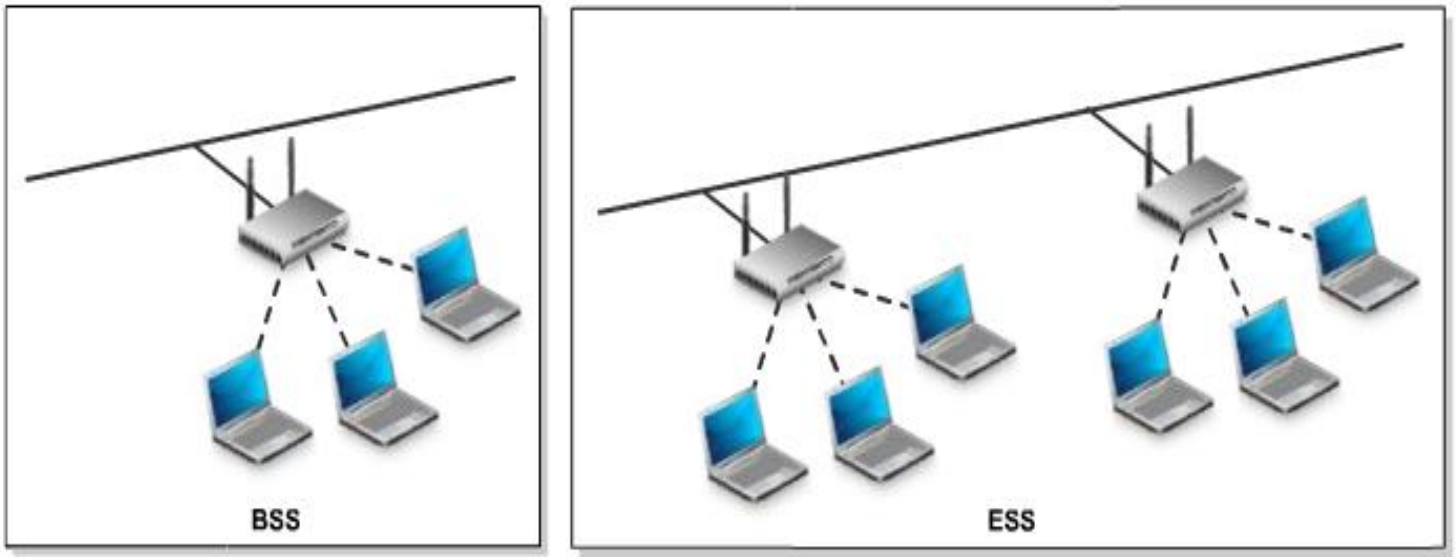
- The wireless **NIC** takes **frames** of data from the link layer, scrambles the data in a predetermined way, then uses the modified data stream to modulate a **radio carrier signal**.

Data Link Layer:

- Uses **C**arriers-**S**ense-**M**ultiple-**A**ccess with **C**ollision **A**voidance (CSMA/CA).

Wireless network implementation

- SSID – (Service Set Identifier of the wireless network)-32 long alfanumeric string identifying the WLAN
- BSS (Basic Service Set) – a network consisting of several clients and a wireless Access Point (AP); unique SSID
- ESS (Extended Service Set) – a network consisting of several wireless AP; adds mobility, Aps can use different SSIDs



IEEE 802.x LAN standards and TCP/IP model

The IEEE 802.x LAN standards deal with the Data Link and Physical layer of the TCP/IP model. IEEE 802.11 only standardizes the physical and medium access control layers in wireless network.



IEEE 802-series of LAN standards

IEEE 802®: Overview & Architecture

IEEE 802.1 ™ Bridging & Management

IEEE 802.2 ™: Logical Link Control

IEEE 802.3 ™: CSMA/CD Access Method

IEEE 802.4 ™: Token-Passing Bus Access Method

IEEE 802.5 ™: Token Ring Access Method

IEEE 802.6 ™: DQDB Access Method

IEEE 802.7 ™: Broadband LAN

IEEE 802.10 ™: Security

IEEE 802.11 ™: Wireless

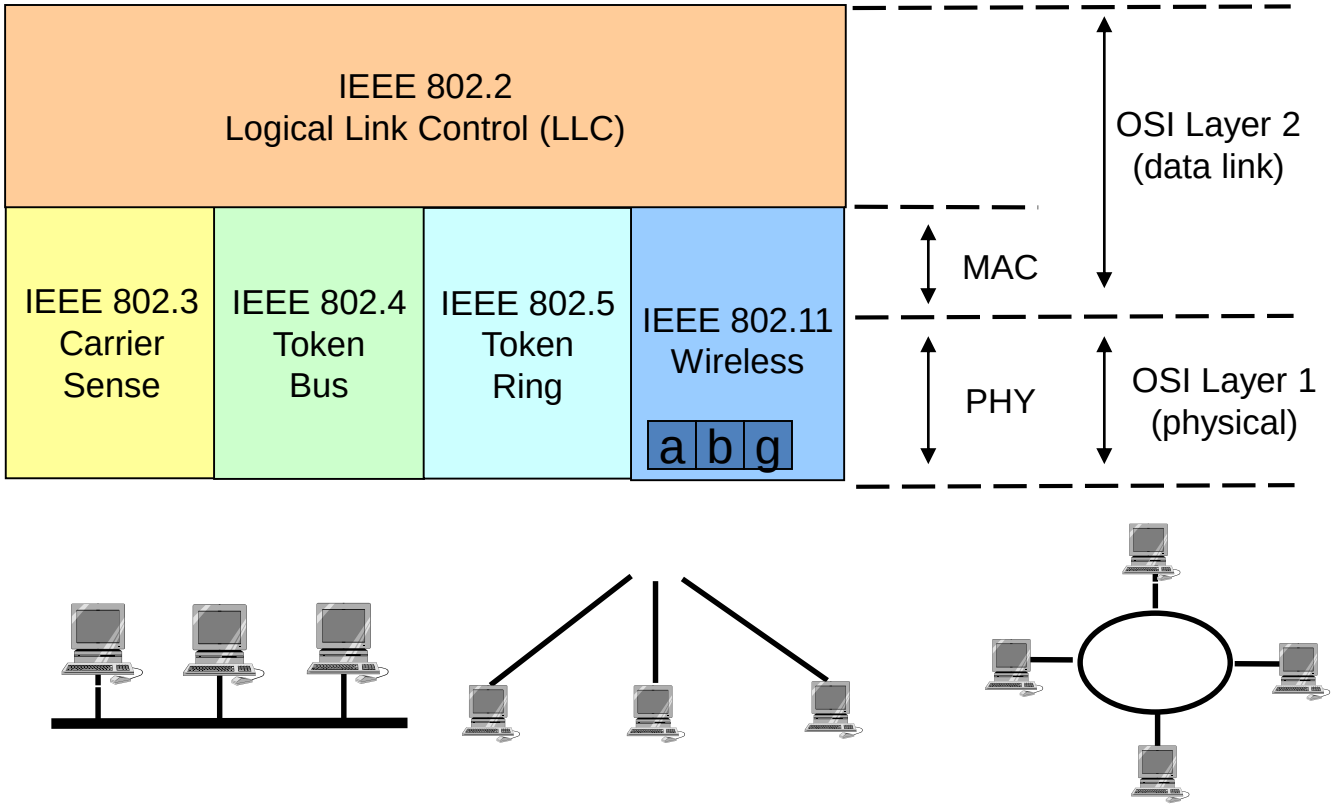
IEEE 802.12 ™: Demand Priority Access

IEEE 802.16™: Broadband Wireless Metropolitan Area Networks

What is 802.11?

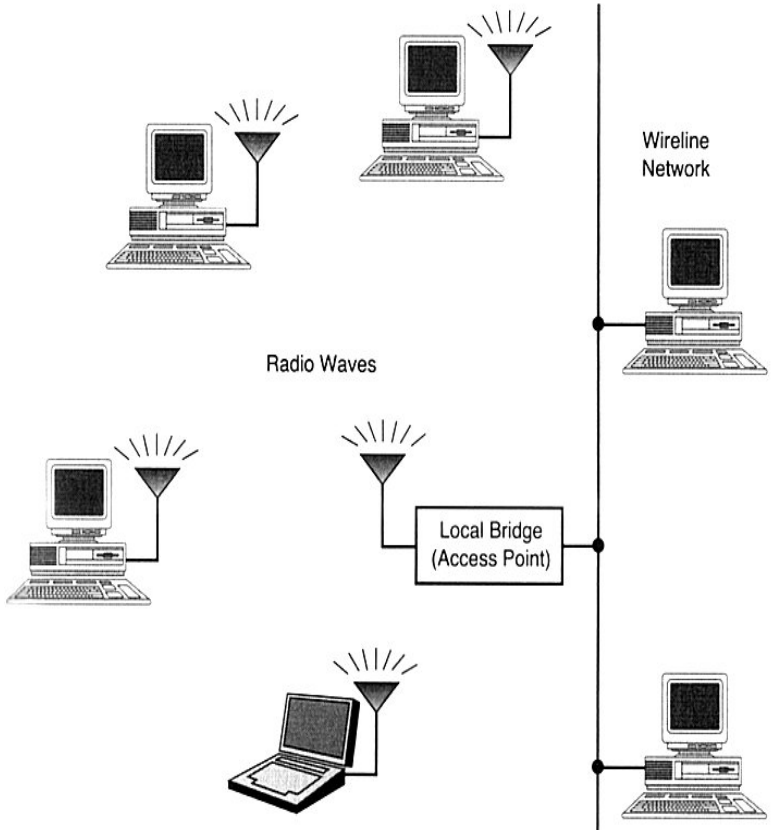
- A family of wireless LAN (WLAN) specifications developed by a working group at the Institute of Electrical and Electronic Engineers (IEEE)
- Defines standard for WLANs using the following four technologies
 - Frequency Hopping Spread Spectrum (FHSS)
 - Direct Sequence Spread Spectrum (DSSS)
 - Infrared (IR)
 - Orthogonal Frequency Division Multiplexing (OFDM)
- Versions: 802.11a, 802.11b, 802.11g, 802.11e, 802.11f, 802.11i

The IEEE 802.11 and supporting LAN Standards



802.11 WLANs - Outline

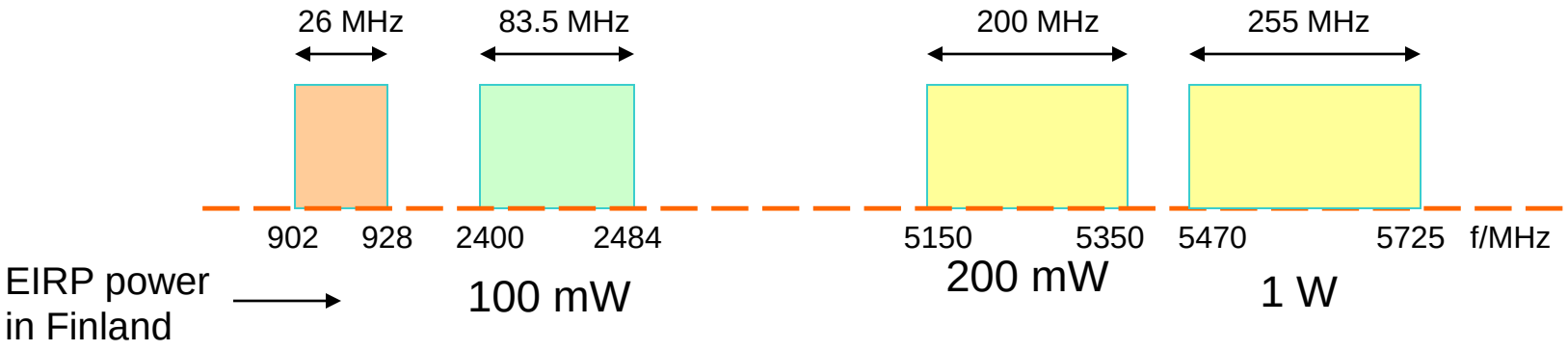
- Media access layer :
 * access to wireless medium
 * authentication & privacy
 * Distributed system:
 _ Association
 – CSMA/CD
- Physical
 – modulation
 - Frequency hopping
 - Direct sequence
 - Infrared



- The 802.11: use five distinct frequency ranges: 2.4 GHz, 3.6 GHz, 4.9 GHz, 5 GHz, and 5.9 GHz bands. Each range is divided into a multitude of channels. Countries apply their own regulations to the allowable channels, allowed users and maximum power levels within these frequency ranges.

802.11 WLAN technologies

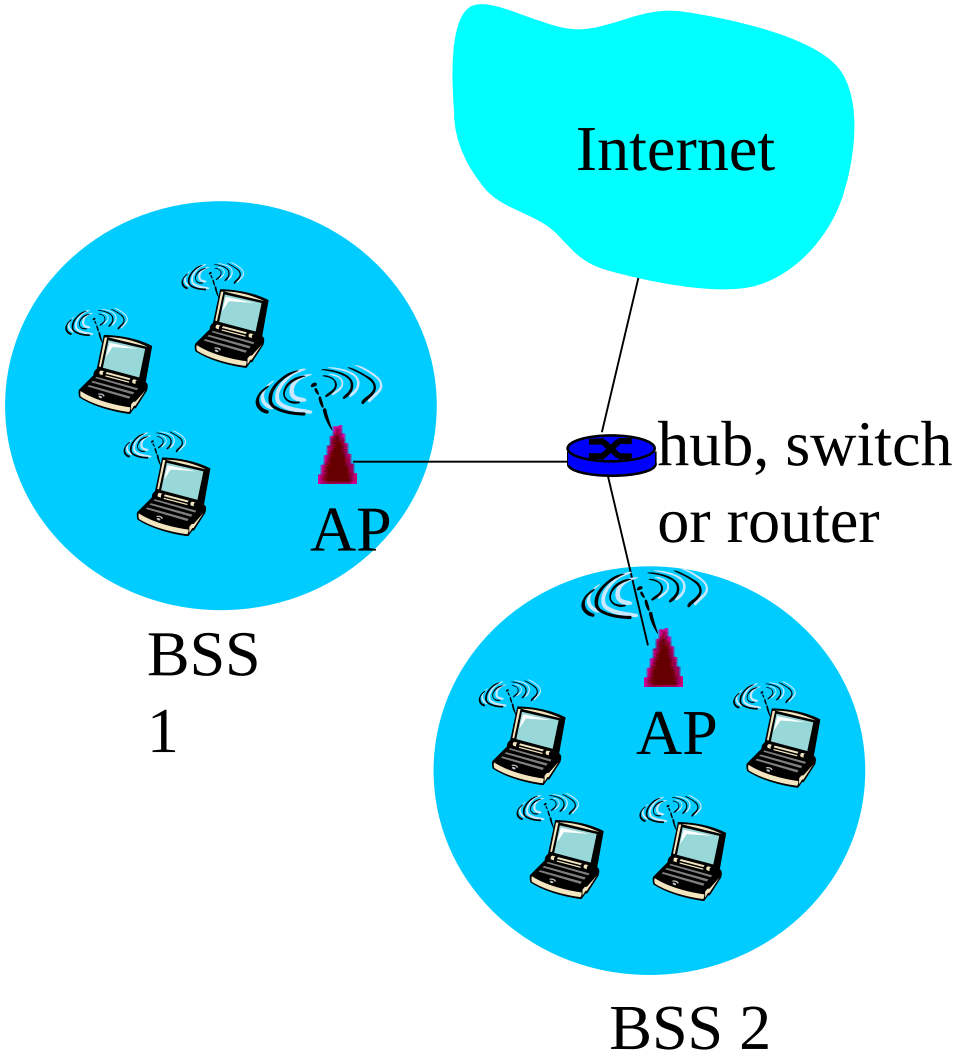
- IEEE 802.11 standards and rates
 - IEEE 802.11 (1997) 1 Mbps and 2 Mbps (2.4 GHz band)
 - IEEE 802.11b (1999) 11 Mbps (2.4 GHz band) = Wi-Fi
 - IEEE 802.11a (1999) 6, 9, 12, 18, 24, 36, 48, 54 Mbps (5 GHz band)
 - IEEE 802.11g (2001 ... 2003) up to 54 Mbps (2.4 GHz) backward compatible to 802.11b
- **IEEE 802.11 networks work on license free industrial, science, medicine (ISM) bands:**



EIRP: Effective Isotropically Radiated Power - radiated power measured immediately after antenna

Equipment technical requirements for radio frequency usage defined in ETS 300 328

802.11 LAN architecture



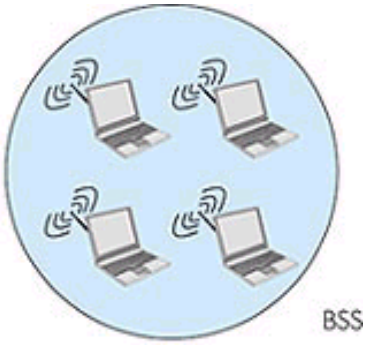
- wireless host communicates with base station
 - base station = access point (AP)
- Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:
 - wireless hosts
 - access point (AP): base station
 - ad hoc mode: hosts only

IEEE 802.11 Architecture

- IEEE 802.11 defines the physical (PHY), and media access control (MAC) layers for a wireless local area network
- 802.11 networks can work as
 - basic service set (BSS)
 - extended service set (ESS)
- BSS can also be used in ad-hoc networking



LLC: Logical Link Control Layer
MAC: Medium Access Control Layer
PHY: Physical Layer
FHSS: Frequency hopping SS
DSSS: Direct sequence SS
SS: Spread spectrum
IR: Infrared light
BSS: Basic Service Set
ESS: Extended Service Set
AP: Access Point
DS: Distribution System



ad-hoc network

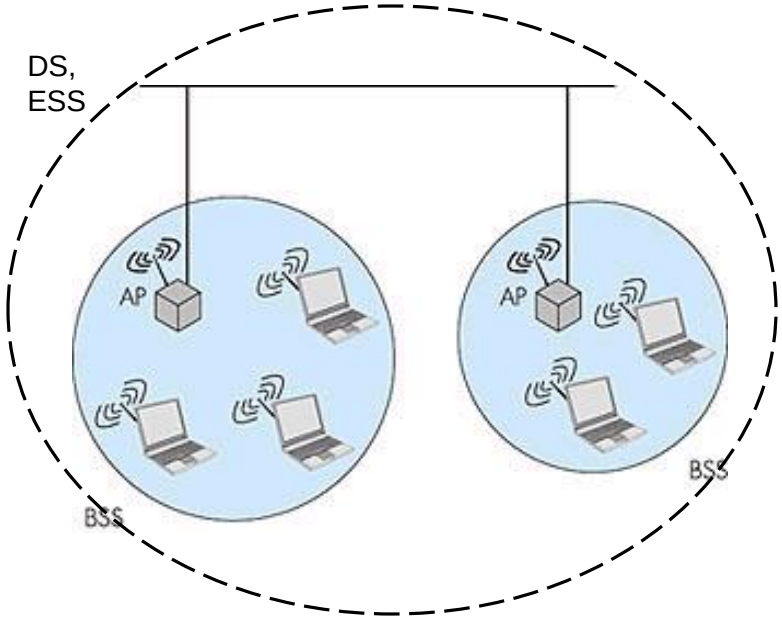


Figure 14.1 *Basic service sets (BSSs)*

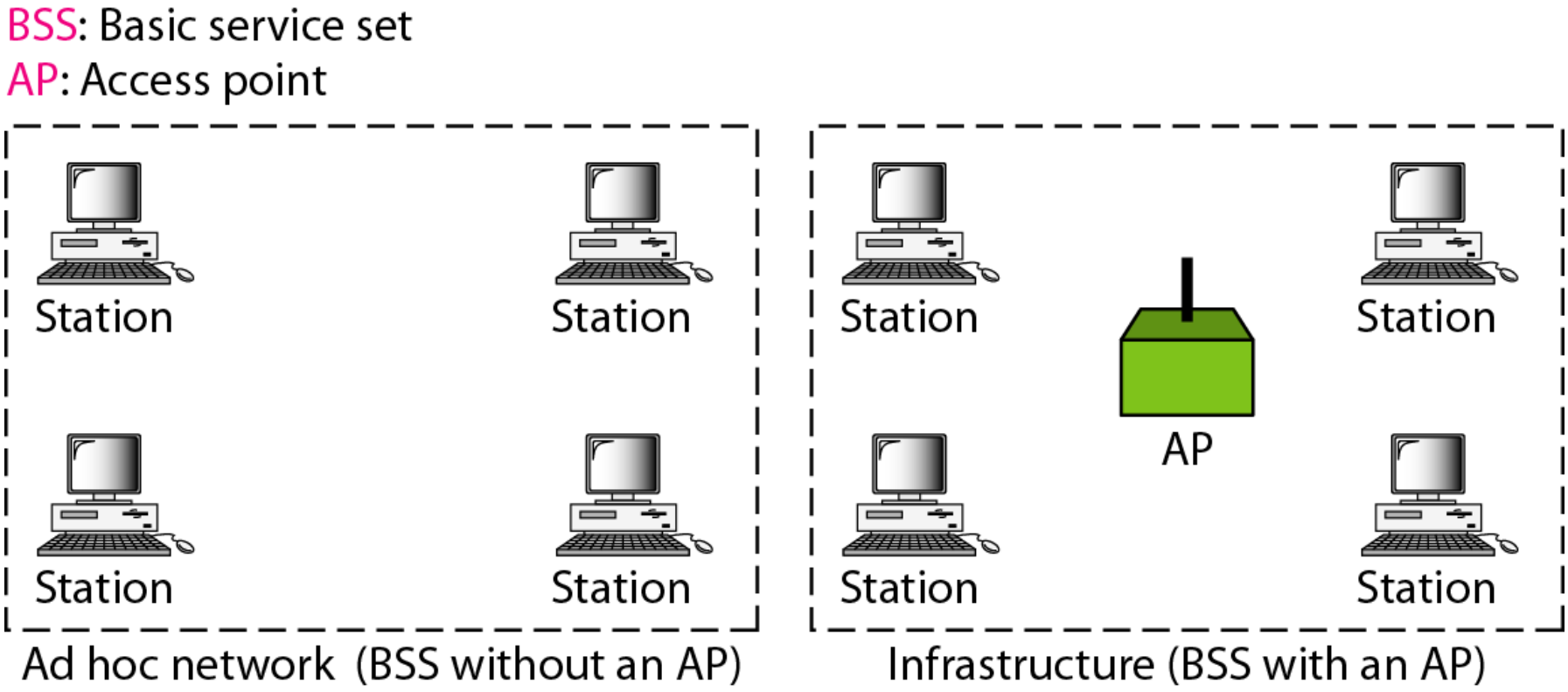
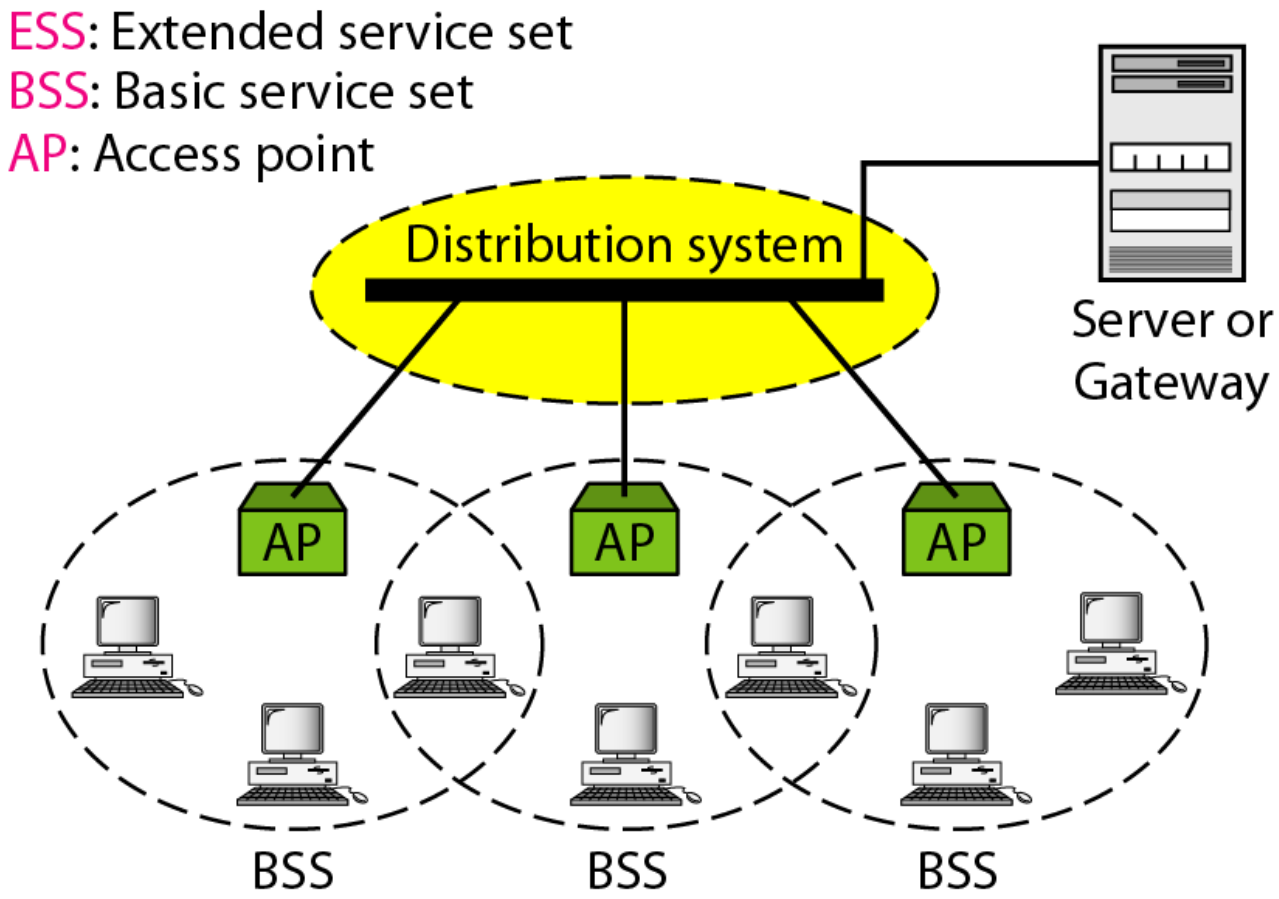
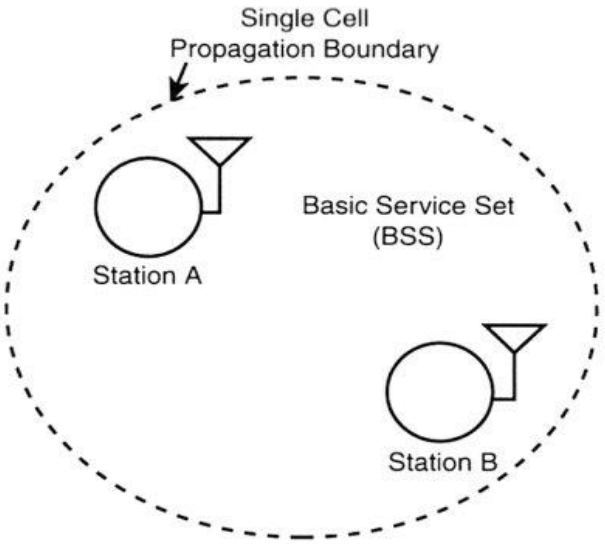


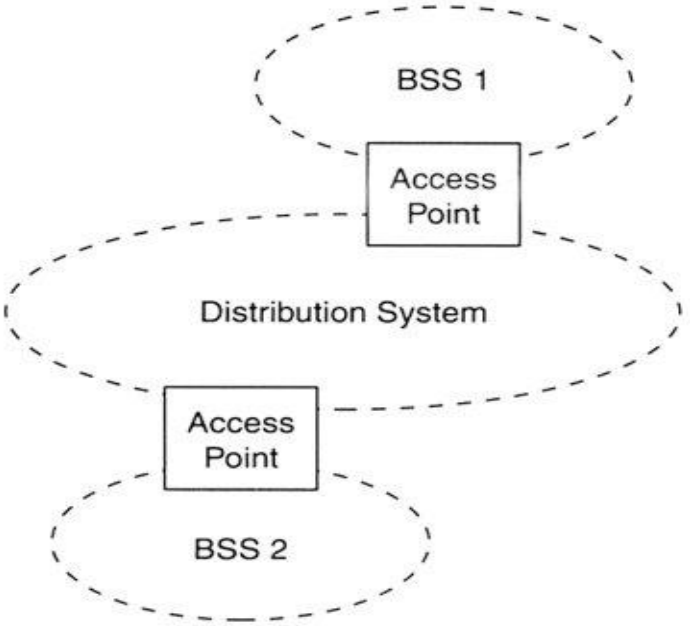
Figure 14.2 *Extended service sets (ESSs)*



BSS and ESS



Basic (independent) service set (BSS)

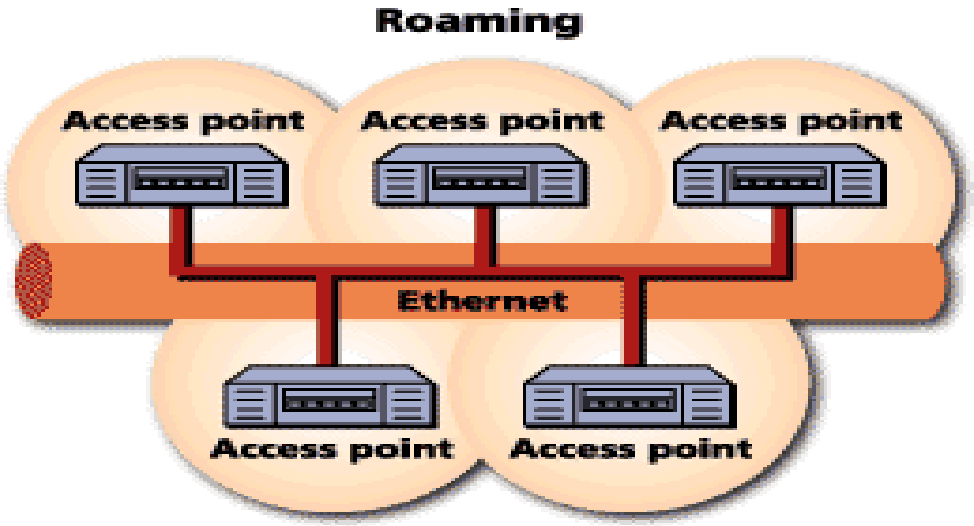


Extended service set (ESS)

- In ESS multiple access points connected by access points and a distribution system as Ethernet
 - BSSs partially overlap
 - Physically disjoint BSSs

Roaming

- Users maintain a continuous connection as they roam from one physical area to another
- Mobile nodes automatically register with the new access point.
- Methods: DHCP, Mobile IP



802.11: Channels, association

- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies.
 - AP admin chooses frequency for AP
 - interference possible: channel can be same as that chosen by neighboring AP!
- host: must *associate* with an AP
 - scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
 - selects AP to associate with
 - may perform authentication
 - will typically run DHCP to get IP address in AP's subnet

802.11 - Transmission

- Most wireless LAN products operate in unlicensed radio bands:
 - 2.4 GHz is most popular
 - Available in most parts of the world
 - No need for user licensing
- Most wireless LANs use spread-spectrum radio
 - Resistant to interference, secure
 - Two popular methods
 - Frequency Hopping (FH)
 - Direct Sequence (DS)

Frequency Hopping Vs. Direct Sequence

- FH systems use a radio carrier that “hops” from frequency to frequency in a pattern known to both transmitter and receiver
 - Easy to implement
 - Resistance to noise
 - Limited throughput (2-3 Mbps @ 2.4 GHz)
- DS systems use a carrier that remains fixed to a specific frequency band. The data signal is spread onto a much larger range of frequencies (at a much lower power level) using a specific encoding scheme.
 - Much higher throughput than FH (11 Mbps)
 - Better range
 - Less resistant to noise (made up for by redundancy – it transmits at least 10 fully redundant copies of the original signal at the same time)

802.11a Vs. 802.11b

802.11a vs. 802.11b	802.11a	802.11b
Raw data rates	Up to 54 Mbps (54, 48, 36, 24,18, 12 and 6 Mbps)	Up to 11 Mbps (11, 5.5, 2, and 1 Mbps)
Range	50 Meters	100 Meters
Bandwidth	UNII and ISM (5 GHz range)	ISM (2.4000—2.4835 GHz range)
Modulation	OFDM technology	DSSS technology

Performance

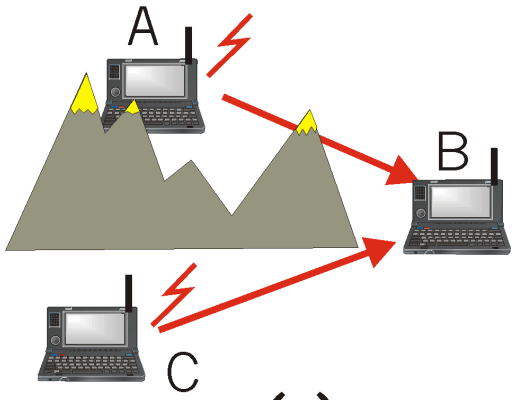
- **802.11a** offers speeds with a theoretically maximum rate of 54Mbps in the 5 GHz band
- **802.11b** offers speeds with a theoretically maximum rate of 11Mbps at in the 2.4 GHz spectrum band
- **802.11g** is a new standard for data rates of up to a theoretical maximum of 54 Mbps at 2.4 GHz.

IEEE 802.11: multiple access

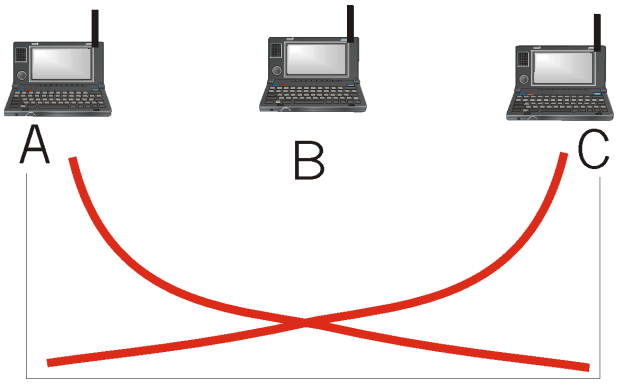
- Avoid collisions: 2 nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
 - don't collide with ongoing transmission by other node
- 802.11: *no* collision detection!
- Over a wired medium like an Ethernet cable it is possible to detect a collision (CD) by measuring the power level on the medium itself. Measuring the power level in a RF environment is not possible with the precision required to detect a packet collision and therefore CD is not possible.
- difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
 - can't sense all collisions in any case: hidden terminal, fading
 - goal: *avoid collisions:* CSMA/C(ollision)A(voidance)

Collision avoidance mechanisms

- Problem:
 - two nodes, hidden from each other, transmit complete frames to base station
 - wasted bandwidth for long duration !
- Solution:
- The fundamental concept in 802.11 MAC to avoid collision is to delay the transmission until medium becomes idle.
 - small reservation packets
 - nodes track reservation interval with internal “network allocation vector” (NAV)

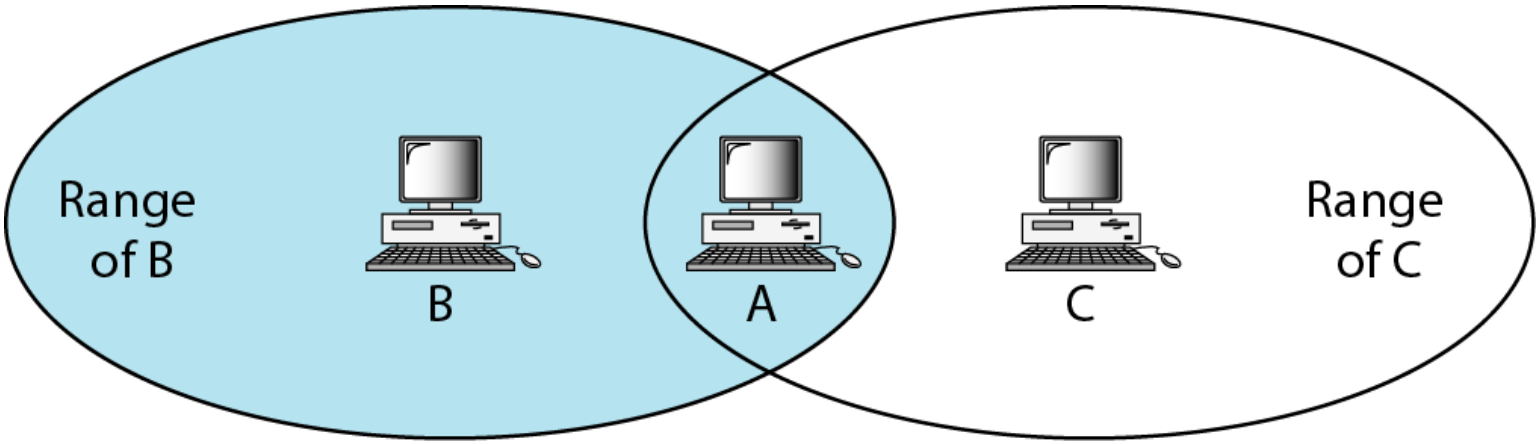


(a)



(b)

Figure 14.10 *Hidden station problem*



Avoiding collisions (more)

idea: allow sender to "reserve" channel rather than random access of data frames: avoid collisions of long data frames

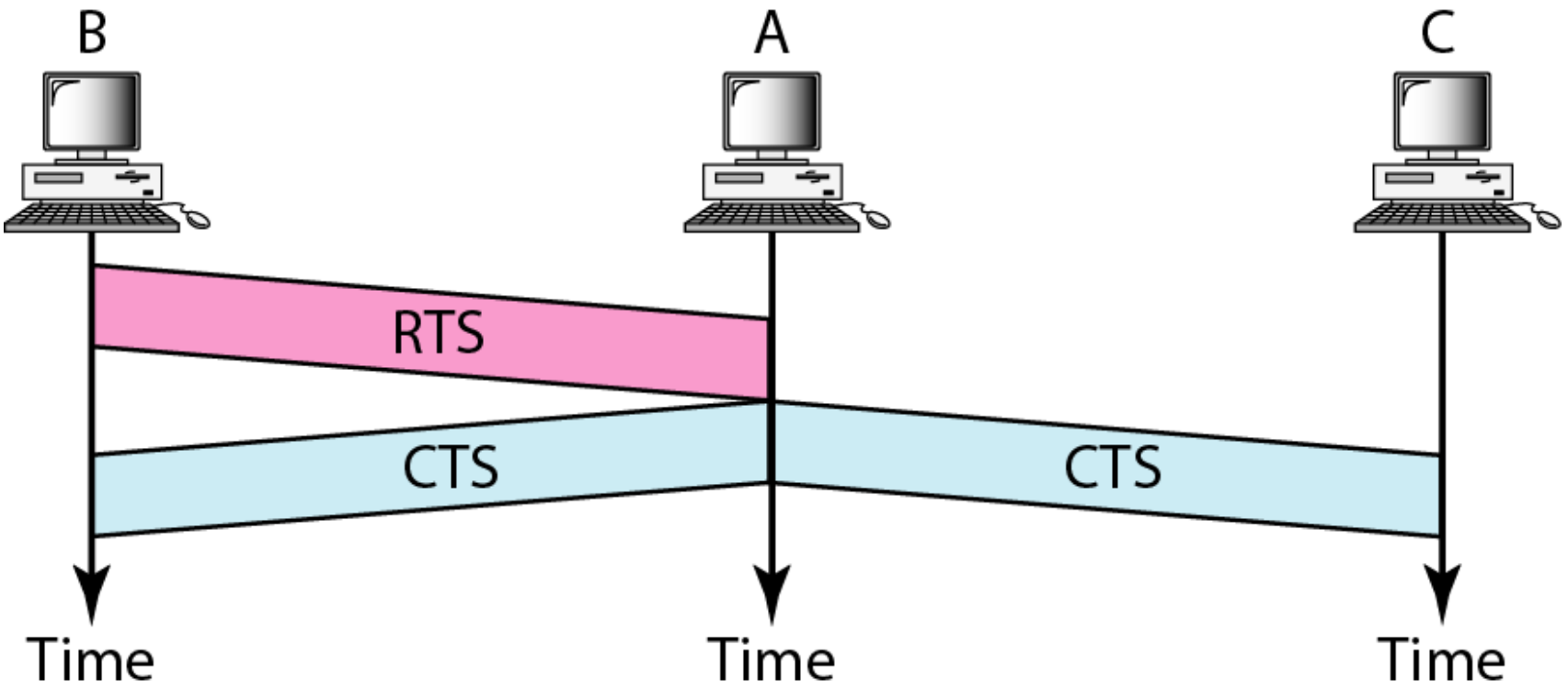
- sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
 - RTSs may still collide with each other (but they're short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
 - sender transmits data frame
 - other stations defer transmissions

avoid data frame collisions completely
using small reservation packets!

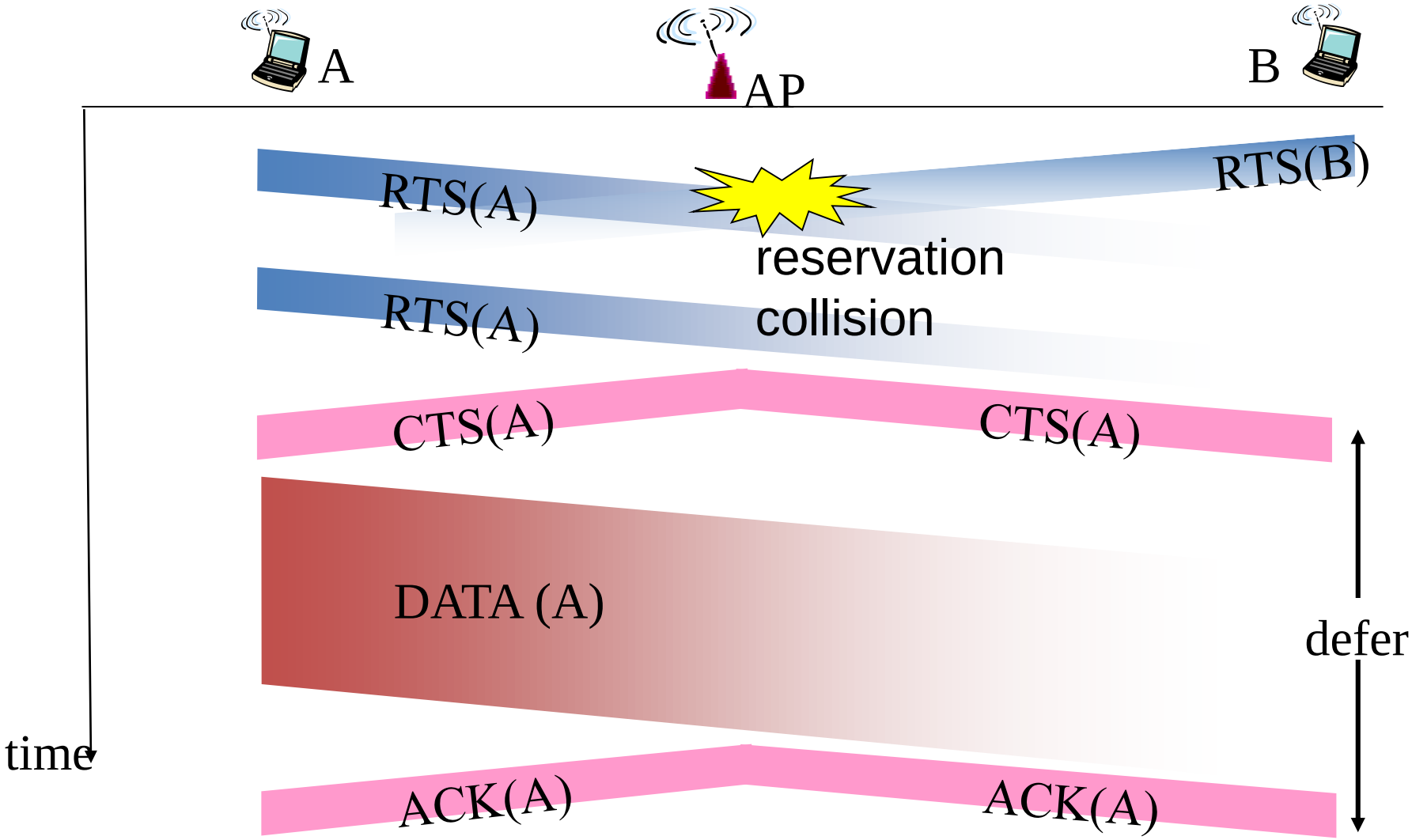
Note

The CTS frame in CSMA/CA handshake can prevent collision from
a hidden station.

Figure 14.11 *Use of handshaking to prevent hidden station problem*



Collision Avoidance: RTS-CTS exchange

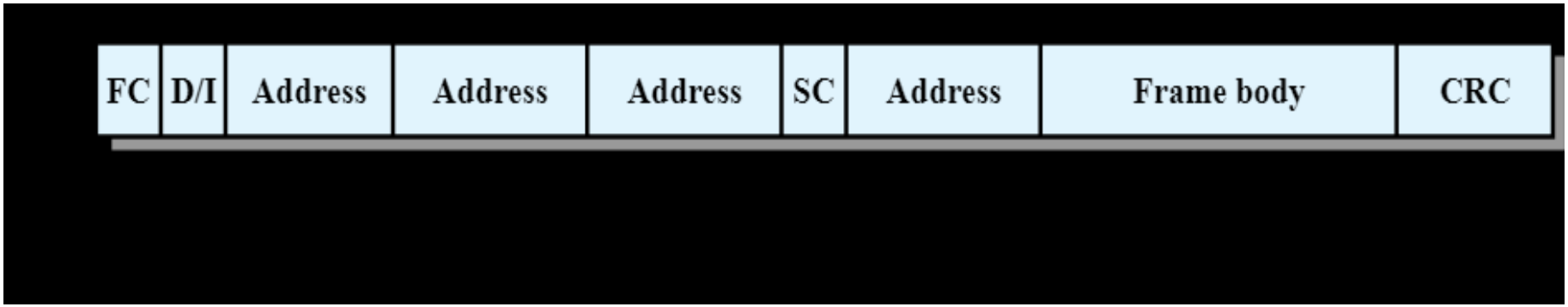


Collision Avoidance: RTS-CTS exchange

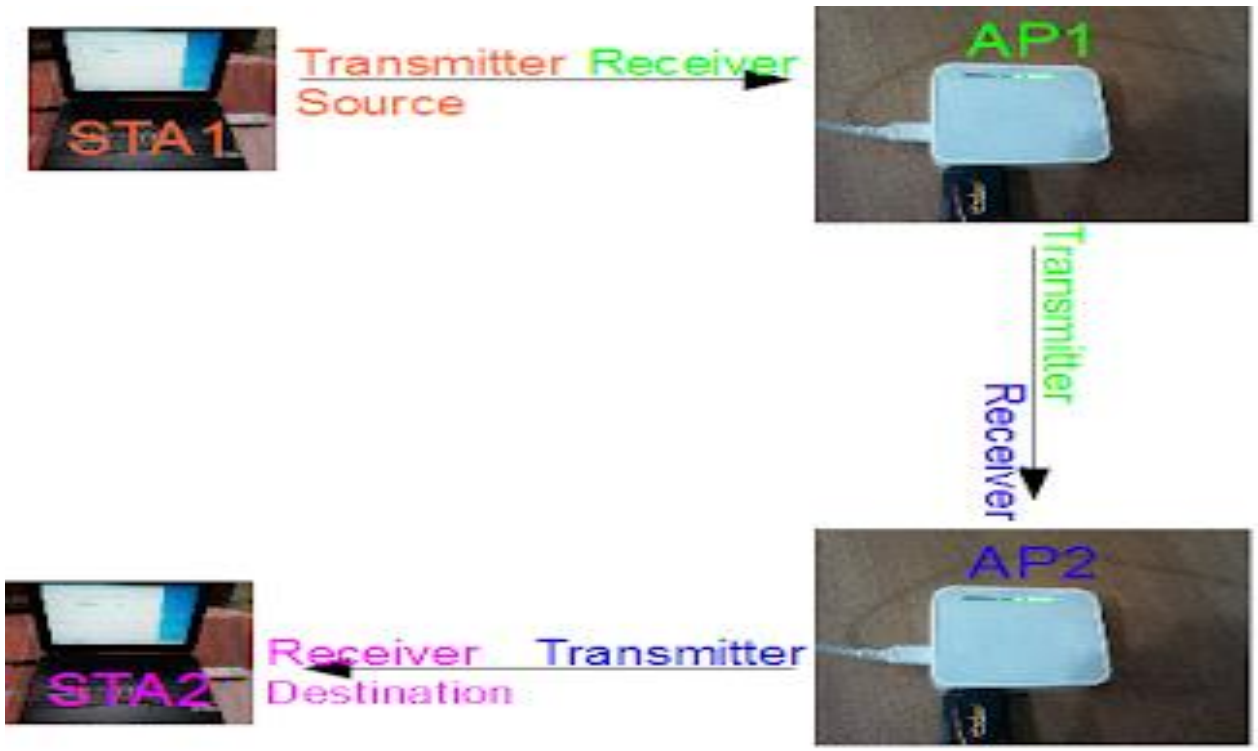
- RTS and CTS short:
 - collisions less likely, of shorter duration
 - end result similar to collision detection
- IEEE 802.11 allows:
 - CSMA
 - CSMA/CA: reservations
 - polling from AP

802.11 frame: addressing

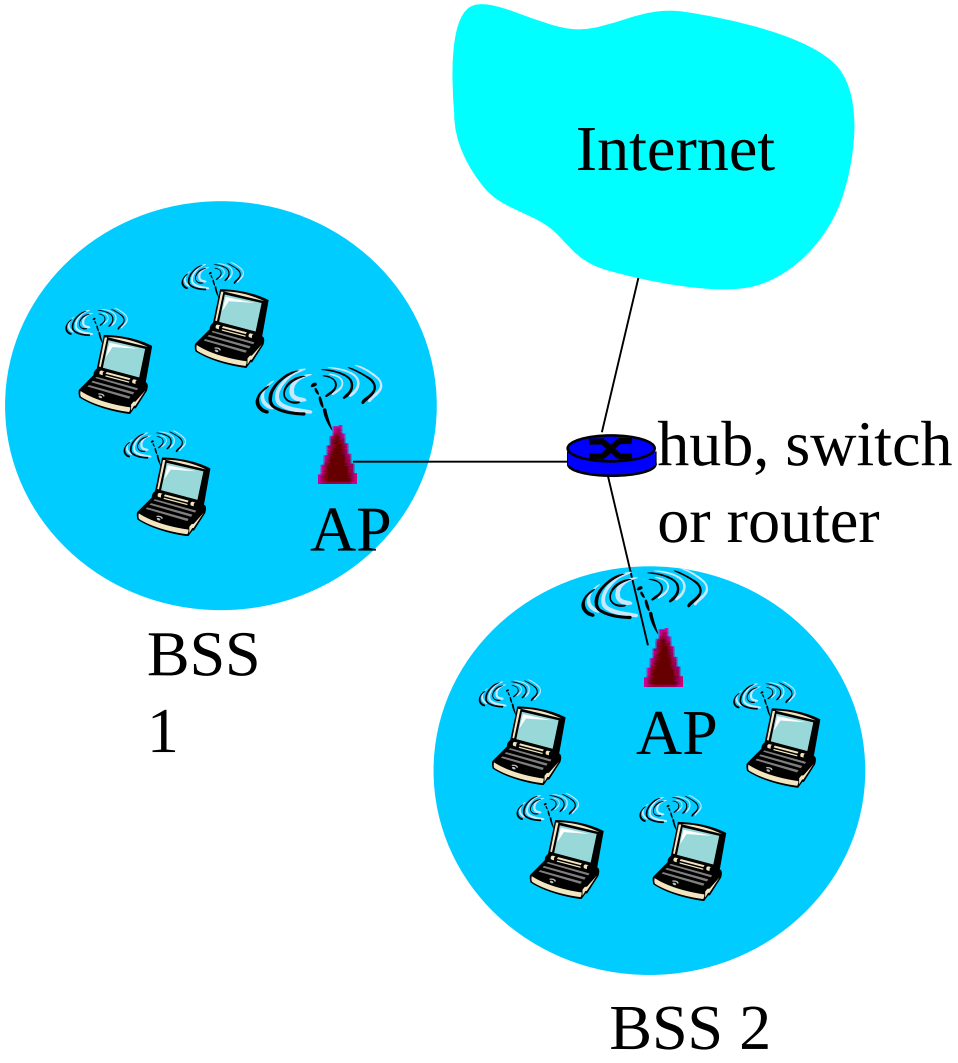
802.11 framing is complex compared to Ethernet framing. This is because the wireless medium requires several management features and frame types not found in wired networks. Address fields are present in the MAC header of 802.11 frames. A frame may contain 4 address fields. Address fields are 6 octets in length. Address fields are used to indicate Source, Transmitter, Destination, Receiver and BSSID.



- **Isn't "Source" same as "Transmitter"? Isn't "Destination" same as "Receiver"?.**
 It depends on the type of frames. They could be same (e.g. in Management frames) or different (in Data frames).



- The above diagram illustrates the difference between various addresses.
- SA(Source Address): Source of the data --> STA1
- TA(Transmitter Address) : STA that transmitted the frame --> STA1, AP1, AP2
- RA(Receiver Address) : Immediate recipient of the frame --> AP1, AP2, STA2
- DA(Destination Address) : Final recipient of the data --> STA2
- BSSID (Basic Service Set IDentifier) : Unique identifier of the BSS, e.g, the MAC address of the AP in an infrastructure network --> AP1, AP2.
- **Are all the 4 address fields always used? No, they are not. Only Address1 is mandatory. For e.g, CTS frame only has Address1. The remaining fields are filled based on the the frame.**



- wireless host communicates with base station
 - base station = access point (AP)
- Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:
 - wireless hosts
 - access point (AP): base station
 - ad hoc mode: hosts only

Table 2: Use of address fields

ToDS	FromDS	Address 1 (receiver)	Address 2 (transmitter)	Address 3	Address 4
0	0	Destination	Source	BSSID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

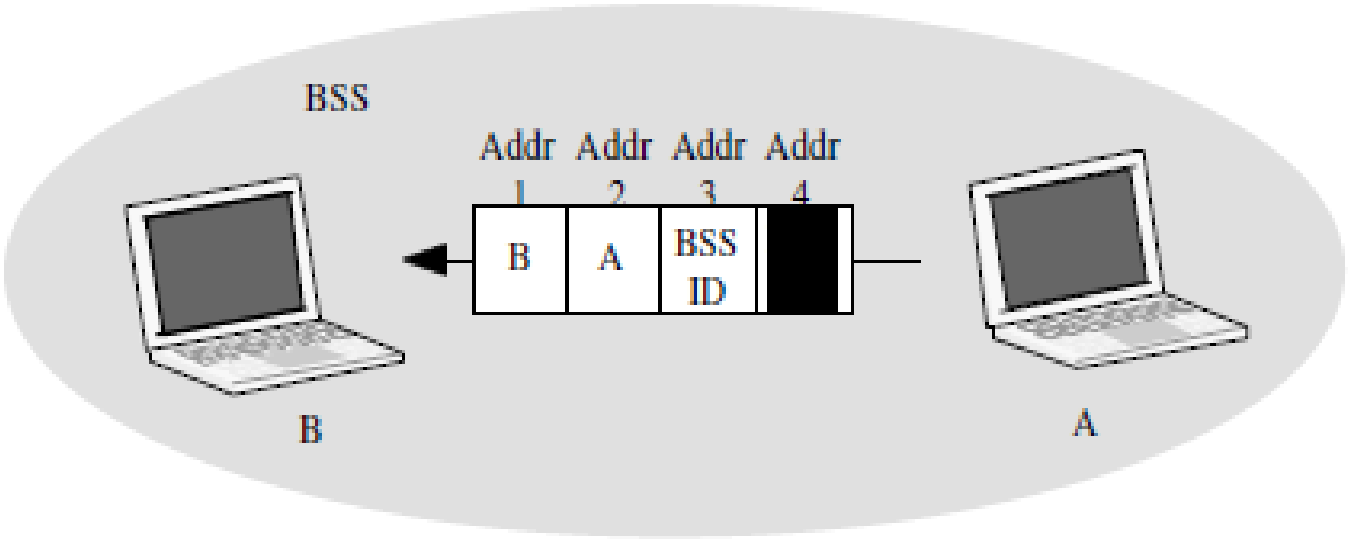


Figure 6: Address field usage in frames in an ad hoc network

Table 2: Use of address fields

ToDS	FromDS	Address 1 (receiver)	Address 2 (transmitter)	Address 3	Address 4
0	0	Destination	Source	BSSID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

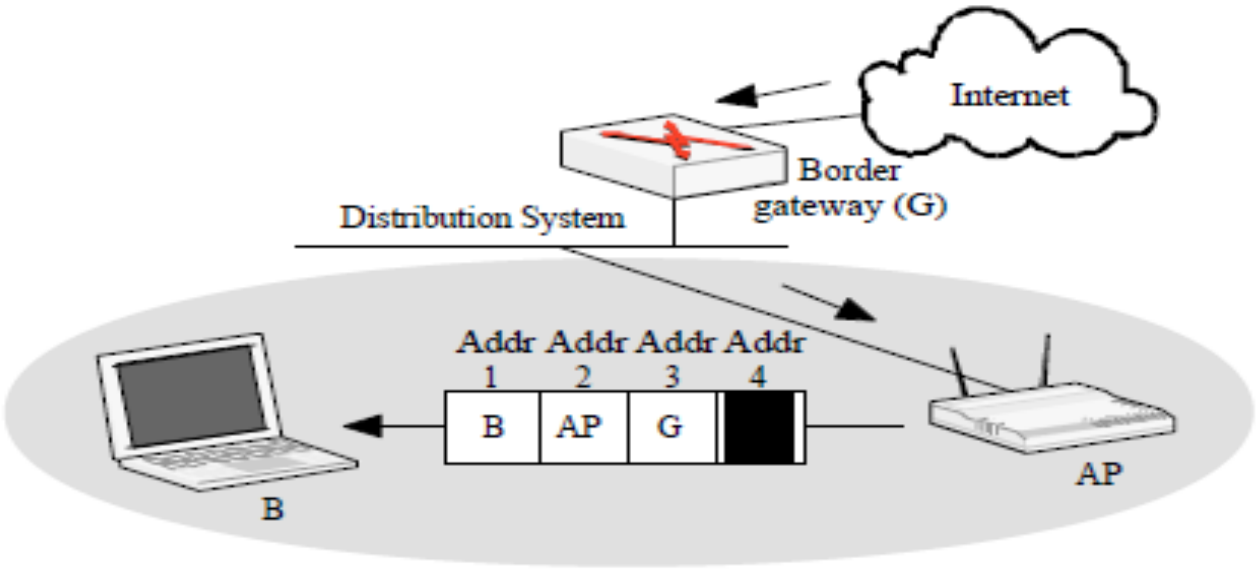
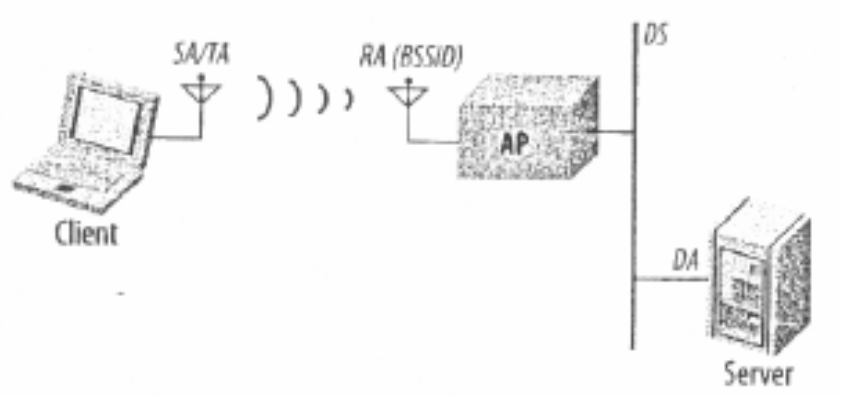


Figure 7: Address field usage in frames from the distribution system

Data frames, to Access Point



- Transmitter = source **but** receiver ≠ destination
- AP's use the third address (DA) to forward the frames

Table 2: Use of address fields

ToDS	FromDS	Address 1 (receiver)	Address 2 (transmitter)	Address 3	Address 4
0	0	Destination	Source	BSSID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

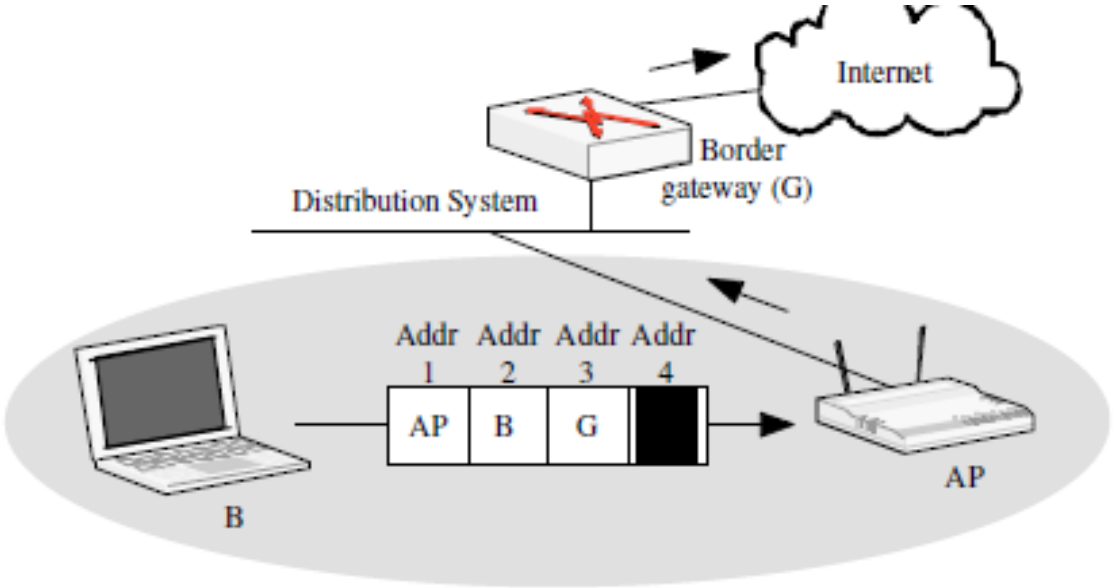
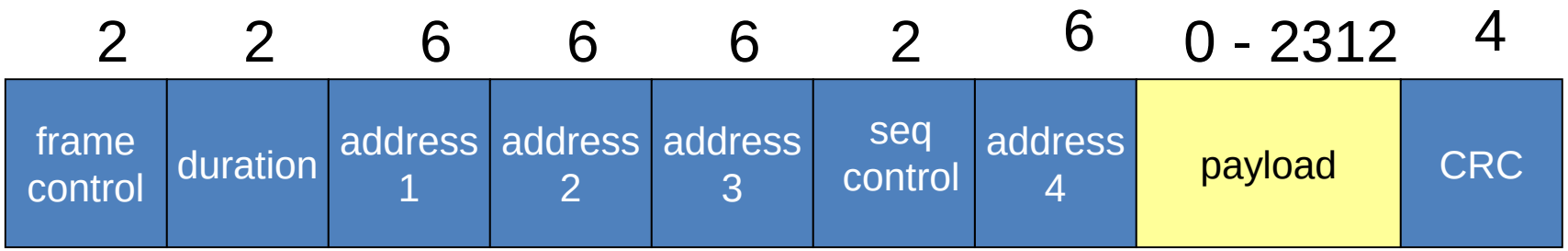


Figure 8: Address field usage in frames to the distribution system

- **Frame Control**: Indicates the type of frame (control, management, or data) and provides control information. Control information includes whether the frame is to or from a DS.
- **Duration/Connection ID**: If used as a duration field, indicates the time (in microseconds) the channel will be allocated for successful transmission of a MAC frame. (the Network Allocation Vector (NAV).
- **Sequence Control**: sequence number used to number frames sent between a given transmitter and receiver.
- **Frame Body**: Contains data unit or MAC control information.
- **Frame Check Sequence**: A 32-bit cyclic redundancy check.



Address 1: MAC address of wireless host or AP to receive this frame

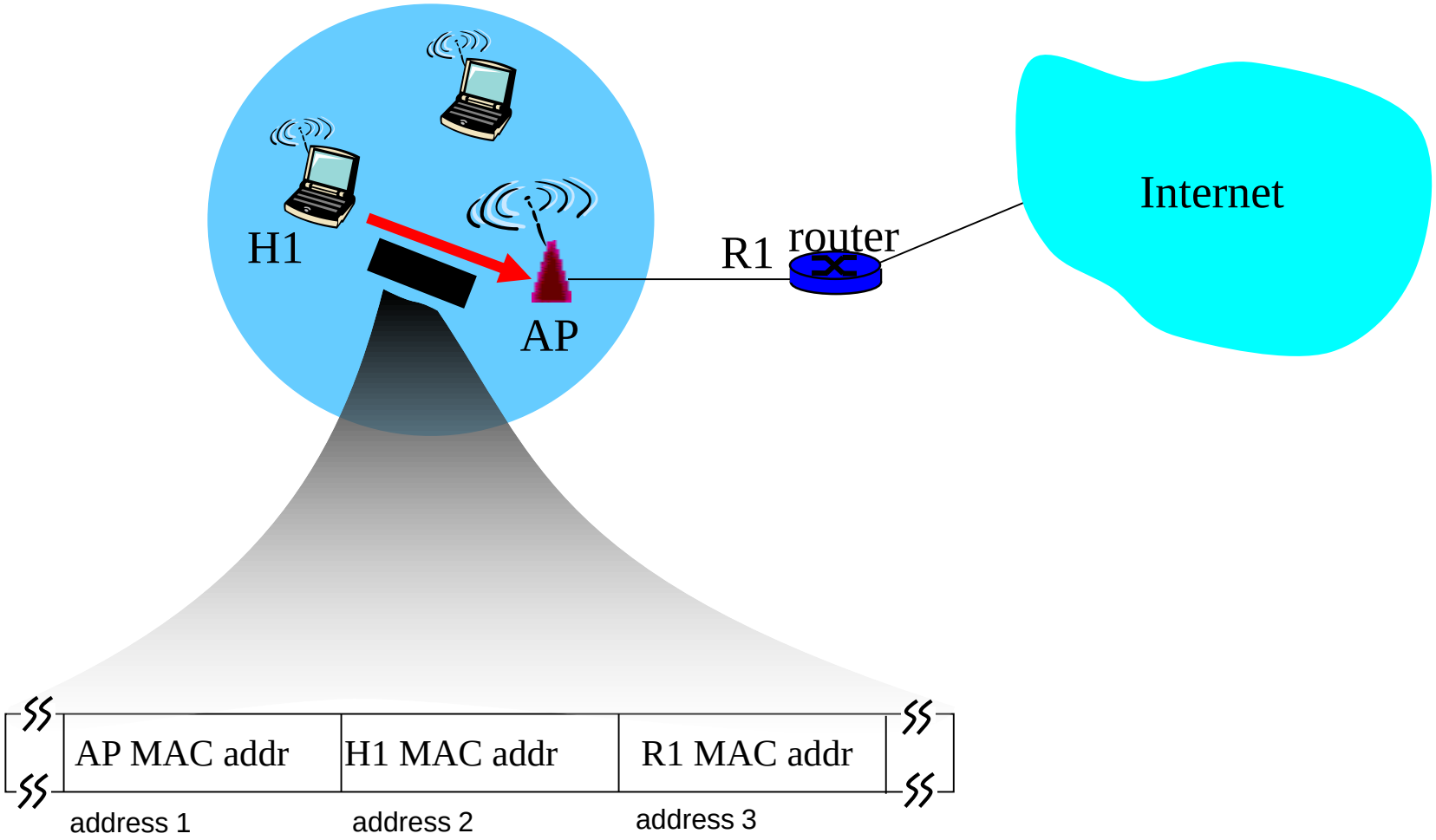
Address 2: MAC address of wireless host or AP transmitting this frame

Address 3: MAC address of router interface to which AP is attached

Address 4

- NOTE: This frame structure is common for all data send by a 802.11 station

TODS=1 and FromDS =0



802.**11** frame

Table 14.4 *Physical layers*

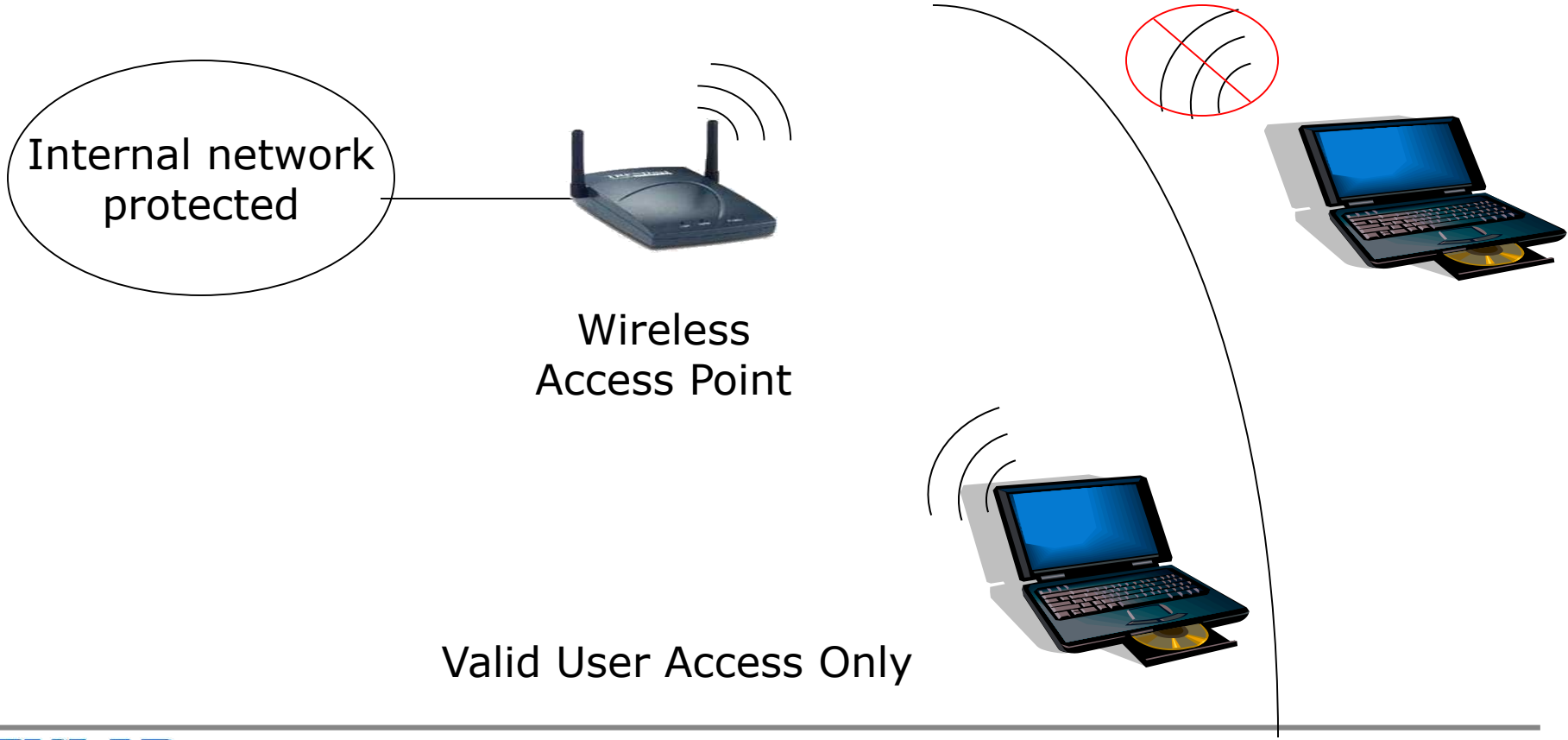
IEEE	*Technique*	*Band*	*Modulation*	*Rate (Mbps)*
802.11	FHSS	2.4 GHz	FSK	1 and 2
	DSSS	2.4 GHz	PSK	1 and 2
		Infrared	PPM	1 and 2
802.11a	OFDM	5.725 GHz	PSK or QAM	6 to 54
802.11b	DSSS	2.4 GHz	PSK	5.5 and 11
802.11g	OFDM	2.4 GHz	Different	22 and 54

Security

- The IEEE 802.11 standard specifies optional security called "**W**ired **E**quivalent **P**rivacy" whose goal is that a wireless LAN offer privacy equivalent to that offered by a wired LAN. The standard also specifies optional authentication measures.

WLAN Security – Problem !!

There is no physical link between the nodes of a wireless network, the nodes transmit over the air and hence anyone within the radio range can eavesdrop on the communication. So conventional security measures that apply to a wired network do not work in this case.



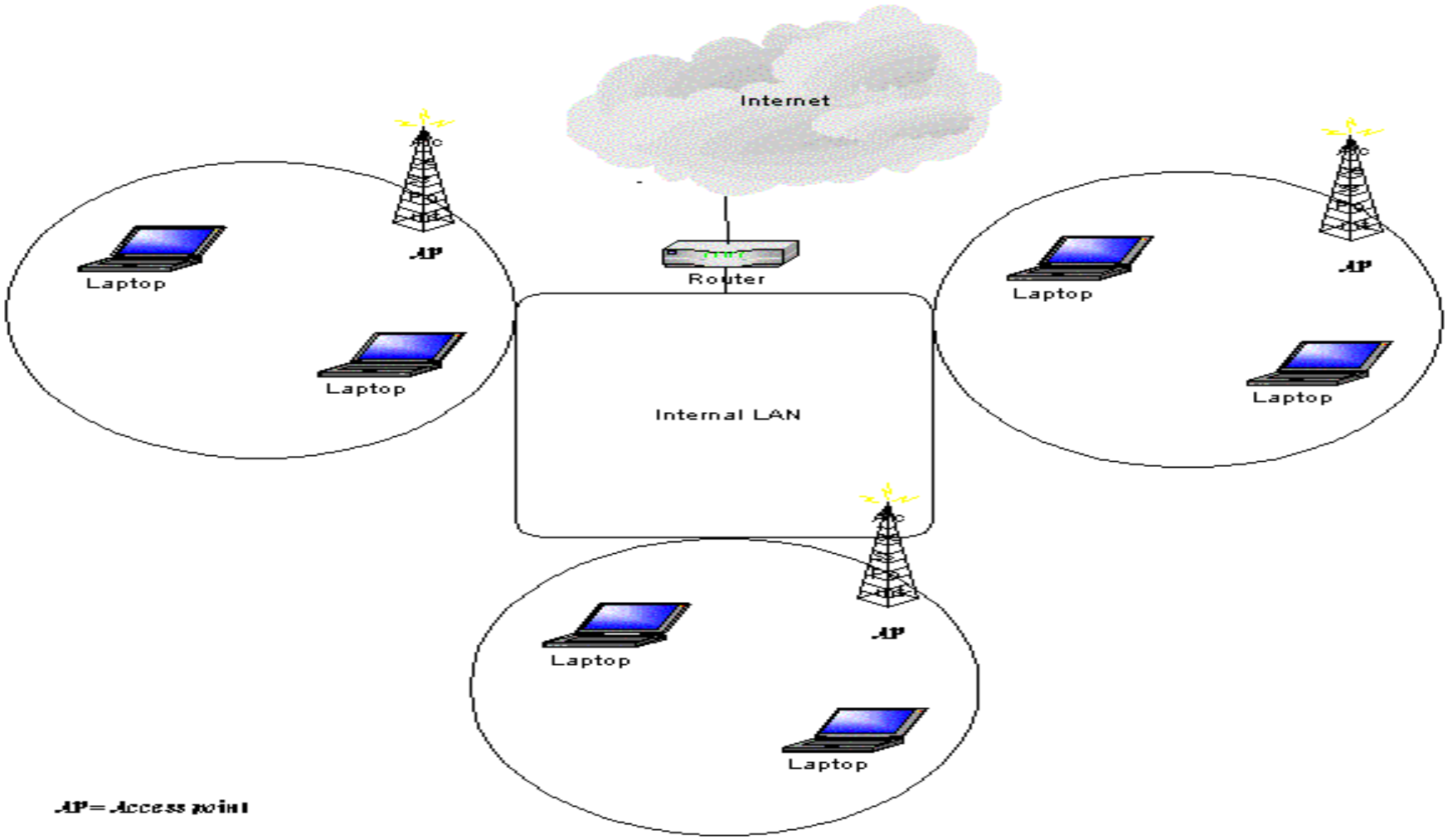
IEEE 802.11 Basic Security Mechanisms

- Service Set Identifier (SSID)
- MAC Address filtering.

- Wired Equivalent Privacy (WEP) protocol

802.11 products are shipped by the vendors with all security mechanisms disabled !!

Wireless network components



Service Set Identifier (SSID) and their limits!

- Limits access by identifying the service area covered by the access points.
- AP periodically broadcasts SSID in a beacon.
- End station listens to these broadcasts and chooses an AP to associate with based upon its SSID.
- Use of SSID – weak form of security as beacon management frames on 802.11 WLAN are always sent in the clear.
- A hacker can use analysis tools (eg. AirMagnet, Netstumbler, AiroPeek) to identify SSID.

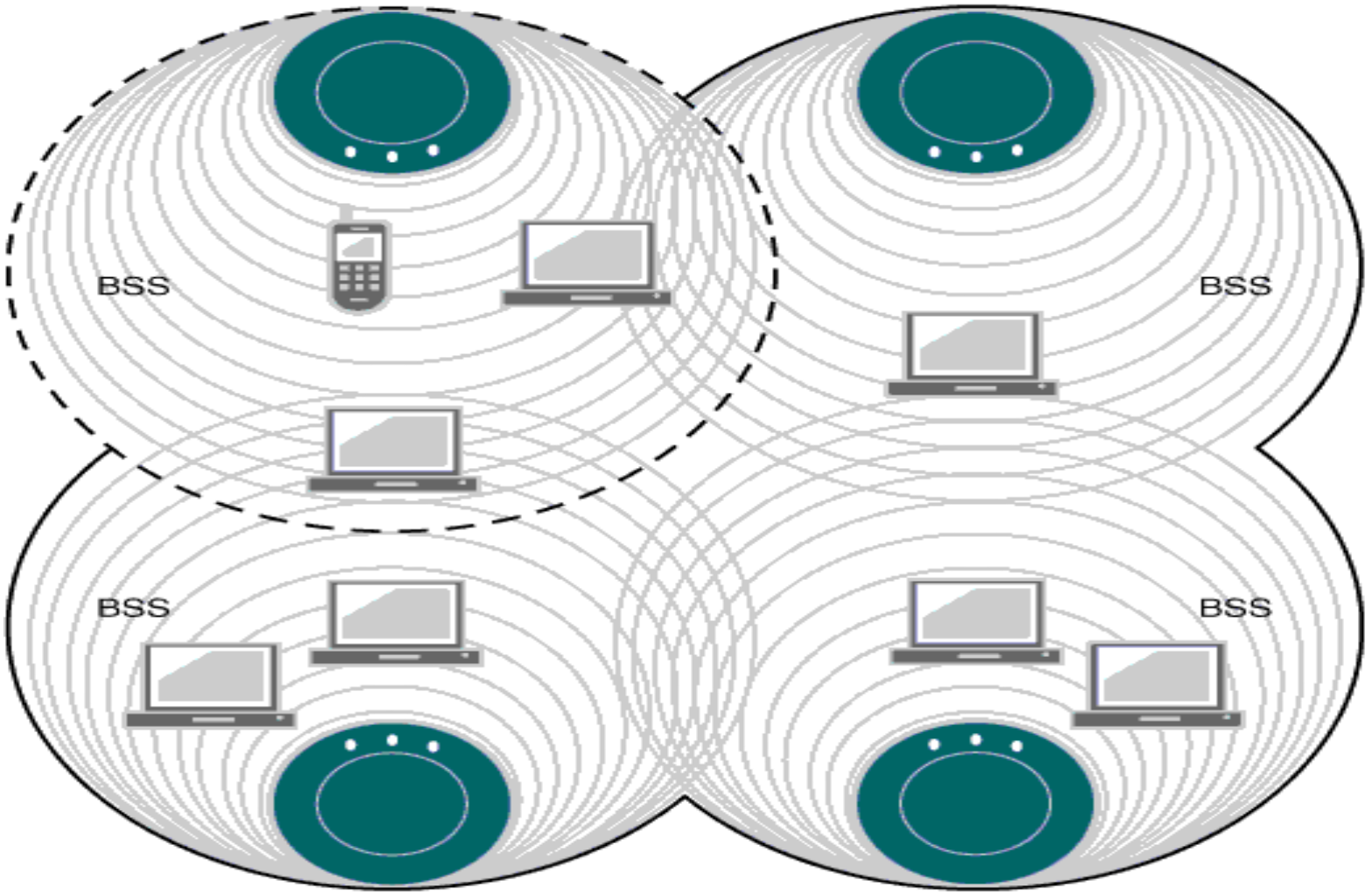
An SSID is the Name of a Network

Because multiple WLANs can coexist in one airspace, each WLAN needs a unique name—this name is the service set ID (SSID) of the network. Your wireless device can see the SSIDs for all available networks—therefore, when you click a wireless icon, the SSIDs recognized by device are listed. For example, suppose your wireless list consists of three SSIDs named Student, Faculty, and Voice. This means that an administrator has created three WLAN Service profiles and, as part of each WLAN service profile, provided the SSID name Student, Faculty, or Voice.

BSSIDs Identify Access Points and Their Clients

Packets bound for devices within the WLAN need to go to the correct destination. The SSID keeps the packets within the correct WLAN, even when overlapping WLANs are present. However, there are usually multiple access points within each WLAN, and there has to be a way to identify those access points and their associated clients. This identifier is called a basic service set identifier (BSSID) and is included in all wireless packets.

BSS+BSS+BSS+BSS=ESS



BSSID = AP MAC address
SSID = name of network

g041300

- **As a user**, you are usually unaware of which basic service set (BSS) you currently belong to. When you physically move your laptop from one room to another, the BSS you use can change because you moved from the area covered by one access point to the area covered by another access point, but this does not affect the connectivity of your laptop.
- **As an administrator**, you are interested in the activity within each BSS. This tells you what areas of the network might be overloaded, and it helps you locate a particular client. By convention, an access point's MAC address is used as the ID of a BSS (BSSID). Therefore, if you know the MAC address, you know the BSSID—and, because all packets contain the originator's BSSID, you can trace a packet. This works fine for an access point with one radio and one WLAN configured.

MAC Address Filtering

The system administrator can specify a list of MAC addresses that can communicate through an access point.

Advantage :

- Provides a little stronger security than SSID

Disadvantages :

- Increases Administrative overhead
- Reduces Scalability

MAC Address

- Can control access by allowing only defined MAC addresses to connect to the network.
- This address can be spoofed.
- Must compile, maintain, and distribute a list of valid MAC addresses to each access point.
- Not a valid solution for public applications

Associating with the AP

- Access points have two ways of initiating communication with a client
- Shared Key or Open Key authentication
- Open key: need to supply the correct SSID
 - Allow anyone to start a conversation with the AP
- Shared Key is supposed to add an extra layer of security by requiring authentication info as soon as one associates

Authentication and privacy

- Goal: to prevent unauthorized access & eavesdropping
- Realized by authentication service prior access
- Open system authentication:
 - When no authentication is required between a wireless client and an access point (AP), open system authentication provides identification of the client by using the wireless adapter's media access control (MAC) address. Open system authentication does not provide authentication. It is merely the default algorithm that Wired Equivalent Privacy(WEP) uses when authentication is not required.

**WEP: Wired Equivalent Privacy*

Open system authentication uses the following process to identify the client:

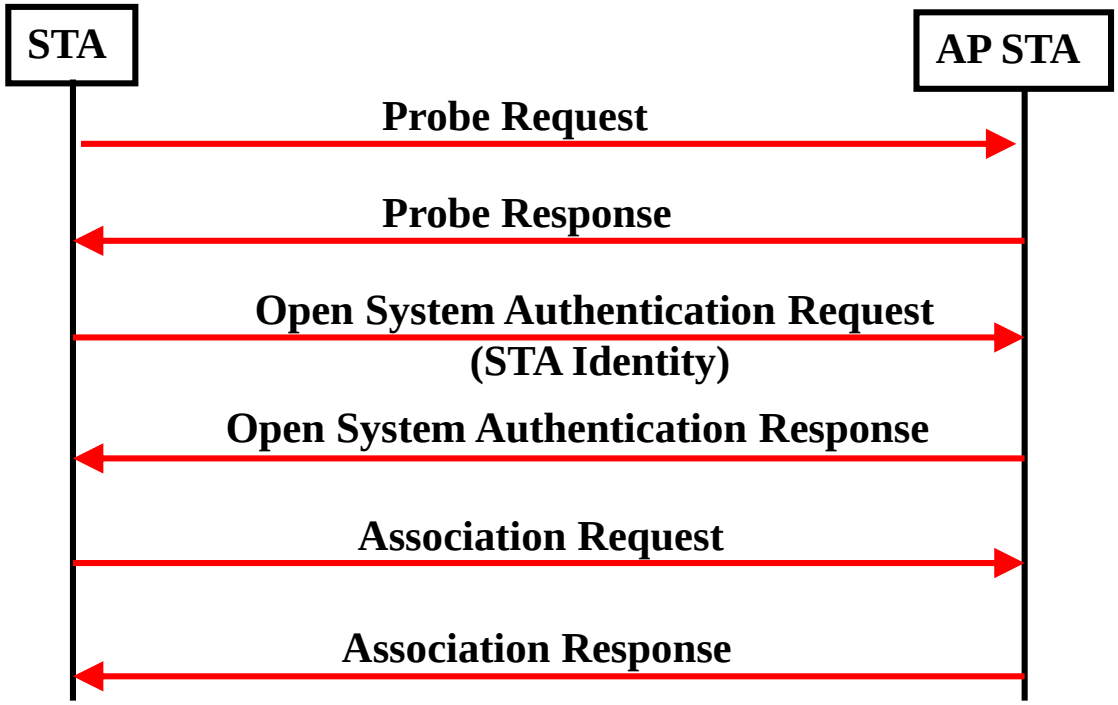
- The wireless client that initiates authentication sends an IEEE 802.11 authentication management frame that contains its identity.
- The receiving wireless AP checks the initiating station's identity and sends back an authentication verification frame.

Open System Authentication (OSA)

- Open System Authentication (OSA) is a process by which a computer can gain access to a wireless network that uses the Wired Equivalent Privacy WEP protocol.
- With OSA, a computer equipped with a wireless modem can access any WEP network and receive files that are not encrypted.
- For OSA to work, the service set identifier (SSID) of the computer should match the SSID of the wireless access point. The SSID is a sequence of characters that uniquely names a wireless local area network (WLAN). The process occurs in three steps:

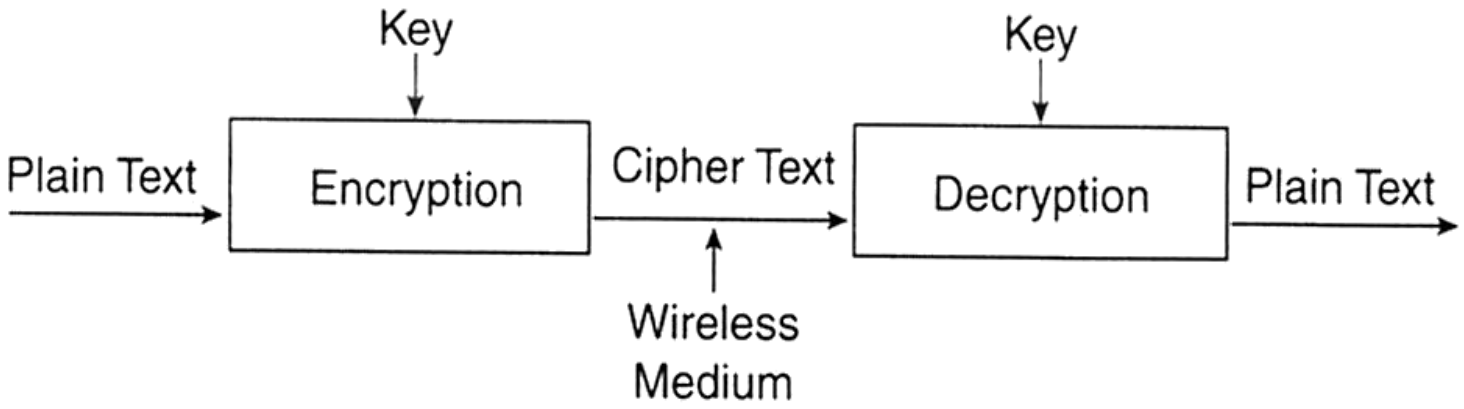
1.Open System Authentication

- Establishing the IEEE 802.11 association with no authentication



- First, the computer sends a request for authentication to the access point.
- Then the access point generates an authentication code, usually at random, intended for use only during that session.
- Finally, the computer accepts the authentication code and becomes part of the network as long as the session continues and the computer remains within range of the original access point.
- If it is necessary to exchange encrypted data between a WEP network access point and a wireless-equipped computer, a stronger authentication process called Shared Key Authentication (SKA) is required.

- Shared key authentication (included in WEP*)
 - **Secret, shared key** received by all stations by a separate, 802.11 independent channel.
 - Stations authenticate by a shared knowledge of the key properties
- WEP's privacy (blocking out eavesdropping) is based on ciphering:

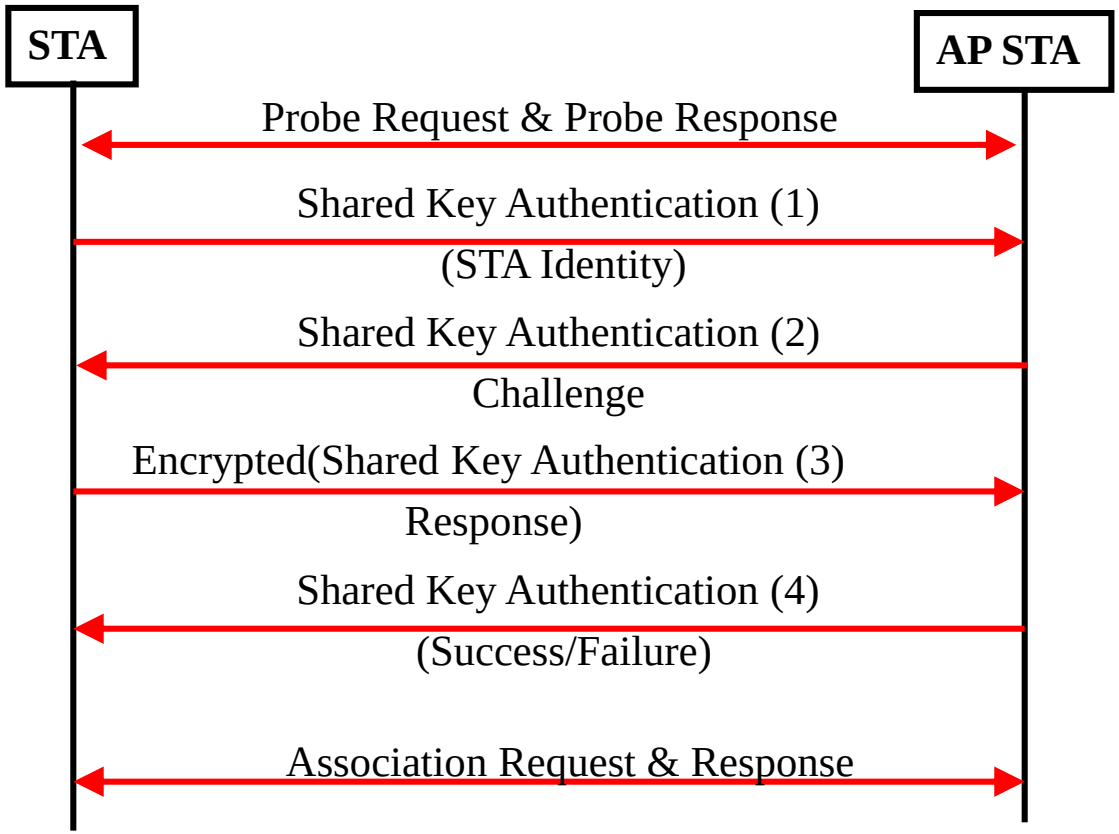


Shared key authentication uses the following process to authenticate a request to connect:

- The wireless client that initiates authentication sends a frame consisting of an identity assertion and a request for authentication.
- The authenticating wireless AP responds to the authentication-initiating wireless node with challenge text.
- The authentication-initiating wireless node replies to the authenticating wireless node with the challenge text that is encrypted using Wired Equivalent Privacy (WEP) and an encryption key that is derived from the shared key authentication secret.
- The authentication result is approved if the authenticating wireless node determines that the decrypted challenge text matches the challenge text originally sent in the second frame. The authenticating wireless node sends the authentication result.

2. Wired Equivalent Privacy (WEP)

- WEP uses shared key authentication



802.11b Security Features

- Wired Equivalent Privacy (**WEP**) – A protocol to protect link-level data during wireless transmission between clients and access points.
- Services:
 - **Authentication**: provides access control to the network by denying access to client stations that fail to authenticate properly.
 - **Confidentiality**: intends to prevent information compromise from casual eavesdropping
 - **Integrity**: prevents messages from being modified while in transit between the wireless client and the access point.

Wired Equivalent Privacy (WEP)

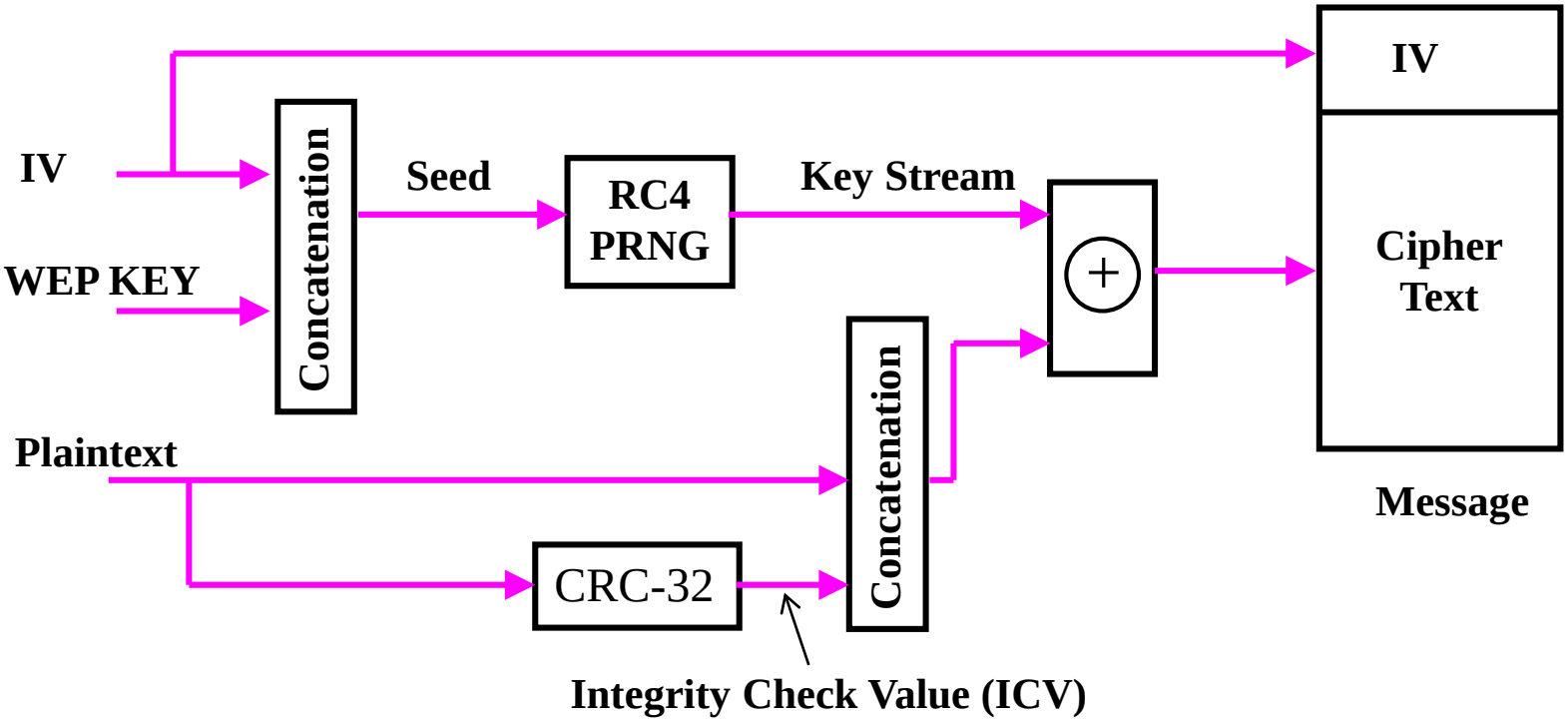
- Designed to provide confidentiality to a wireless network similar to that of standard LANs.
- WEP is essentially the RC4 symmetric key cryptographic algorithm (same key for encrypting and decrypting).
- Transmitting station concatenates 40 bit key with a 24 bit Initialization Vector (IV) to produce pseudorandom key stream.
- Plaintext is XORed with the pseudorandom key stream to produce ciphertext.
- Ciphertext is concatenated with IV and transmitted over the Wireless Medium.
- Receiving station reads the IV, concatenates it with the secret key to produce local copy of the pseudorandom key stream.
- Received ciphertext is XORed with the key stream generated to get back the plaintext.

Wired Equivalent Protocol (WEP)

- Primary built security for 802.11 protocol
- Uses 40bits to 128bits RC4 encryption
- RC4 symmetric key, stream cipher algorithm to generate a pseudo random data sequence. The stream is XORed with the data to be transmitted
- Unfortunately, since ratification of the 802.11 standard, RC4 has been proven insecure, leaving the 802.11 protocol wide open for attack

2. Wired Equivalent Privacy (WEP)

- WEP Encryption uses RC4 stream cipher



Data Integrity

- Data integrity is ensured by a simple encrypted version of CRC (Cyclic Redundant Check)

2. Wired Equivalent Privacy (WEP)

- Several major problems in WEP security
 - The IV used to produce the RC4 stream is only 24-bit long
 - The short IV field means that the same RC4 stream will be used to encrypt different texts – IV collision
 - Statistical attacks can be used to recover the plaintexts due to IV collision
 - The CRC-32 checksum can be easily manipulated to produce a valid integrity check value (ICV) for a false message

More secure is WPA---Wireless Protected Access